



オブジェクトの処理

StorageGRID 11.5

NetApp
April 11, 2024

目次

オブジェクトの処理	1
S3 オブジェクトロックを使用する	5
サーバ側の暗号化を使用	7
オブジェクトの取得	9
HEAD Object の実行	12
POST Object restore の実行	14
PUT Object の場合	16
PUT Object - Copy の各コマンドを実行します	20

オブジェクトの処理

このセクションでは、StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

- "S3 オブジェクトロックを使用する"
- "サーバ側の暗号化を使用する"
- "オブジェクトの取得"
- "HEAD Object の実行"
- "POST Object restore の実行"
- "PUT Object の場合"
- "PUT Object - Copy の各コマンドを実行します"

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID 整合性制御は、次の点を除いて、オブジェクトに対するすべての処理でサポートされます。
 - GET Object ACL の場合
 - OPTIONS /
 - オブジェクトのリーガルホールドを適用します
 - PUT Object retention のことです
- 同一キーに書き込む2つのクライアントなど競合するクライアント要求は最新のWINS形式で解決されま
す「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではな
く、StorageGRID システムが特定の要求を完了したタイミングに基づいています。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも
含めて、すべてバケット所有者によって所有されます。
- Swift を使用して StorageGRID システムに取り込まれたデータオブジェクトに S3 を使用してアクセスす
ることはできません。

次の表に、StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

操作	実装
オブジェクトを削除します	<p>多要素認証 (MFA) と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>StorageGRID は、DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとしています。成功すると、StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。</p> <ul style="list-style-type: none"> バージョン管理 * <p>特定のバージョンを削除するには、バケットの所有者を要求元にしてを使用する必要があります <code>versionId</code> サブリソース：このサブリソースを使用すると、バージョンが完全に削除されます。状況に応じて <code>versionId</code> 削除マーカー、応答ヘッダーに対応します <code>x-amz-delete-marker</code> はに設定されています <code>true</code>。</p> <ul style="list-style-type: none"> を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが有効になっているバケットのサブリソースが表示されると、削除マーカーが生成されます。。 <code>versionId</code> 削除マーカーの場合は、を使用して戻ります <code>x-amz-version-id</code> 応答ヘッダー、および <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが一時停止中のバケットについて、既存の「null」バージョンまたは「null」削除マーカーが完全に削除され、新しい「null」削除マーカーが生成されます。。 <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 注*：特定の場、1つのオブジェクトに複数の削除マーカーが存在することがあります。
複数のオブジェクトを削除します	<p>多要素認証 (MFA) と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>同じ要求メッセージで複数のオブジェクトを削除できます。</p>

操作	実装
オブジェクトのタグ付けを削除します	<p>を使用します tagging サブリソース：オブジェクトからすべてのタグを削除します。Amazon S3 REST API のすべての動作が実装されています。</p> <ul style="list-style-type: none"> バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合 は、"MethodNotAllowed"ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
オブジェクトの取得	"オブジェクトの取得"
GET Object ACL の場合	アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID、表示名、および権限が表示されます。
オブジェクトのリーガルホールドを取得します	"S3 オブジェクトロックを使用する"
GET Object retention のことです	"S3 オブジェクトロックを使用する"
GET Object tagging	<p>を使用します tagging サブリソース：オブジェクトのすべてのタグを返すために使用します。Amazon S3 REST API のすべての動作が実装されています</p> <ul style="list-style-type: none"> バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合、"MethodNotAllowed"ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
HEAD Object の実行	"HEAD Object の実行"
POST Object restore の実行	"POST Object restore の実行"
PUT Object の場合	"PUT Object の場合"

操作	実装
PUT Object - Copy の各コマンドを実行します	"PUT Object - Copy の各コマンドを実行します"
オブジェクトのリーガルホールドを適用します	"S3 オブジェクトロックを使用する"
PUT Object retention のことです	"S3 オブジェクトロックを使用する"
PUT Object tagging	<p>を使用します tagging サブリソース：既存のオブジェクトに一連のタグを追加します。Amazon S3 REST API のすべての動作が実装されています</p> <ul style="list-style-type: none"> • タグの更新と取り込み動作 * <p>PUT Object tagging を使用してオブジェクトのタグを更新した場合、StorageGRID はオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。</p> <p>このため、ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。</p> <ul style="list-style-type: none"> • 衝突の解決 * <p>同一キーに書き込む2つのクライアントなど競合するクライアント要求は最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。</p> <ul style="list-style-type: none"> • バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていません。処理は、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグを追加します。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed" ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>

関連情報

"整合性制御"

S3 オブジェクトロックを使用する

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、S3 オブジェクトのロックを有効にしたバケットを作成し、そのバケットに追加するオブジェクトのバージョンごとに retain-until date および legal hold 設定を指定できます。

S3 オブジェクトロックでは、オブジェクトレベルの設定を指定して、一定期間または無期限にオブジェクトが削除または上書きされないようにすることができます。

StorageGRID S3 オブジェクトロック機能は、Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

バケットでS3オブジェクトのロックを有効にする

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。次のいずれかの方法を使用できます。

- Tenant Manager を使用してバケットを作成します。

"テナントアカウントを使用する"

- を指定したPUT Bucket要求を使用してバケットを作成します x-amz-bucket-object-lock_enabled 要求ヘッダー。

"バケットの処理"

バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。

S3 オブジェクトのロックが有効になっているバケットには、S3 オブジェクトのロック設定があるオブジェクトとなっていないオブジェクトを組み合わせる含めることができます。StorageGRID では、S3オブジェクトロックバケット内のオブジェクトのデフォルトの保持はサポートされないため、PUT Object Lock Configurationバケットの処理はサポートされません。

バケットでS3オブジェクトのロックが有効になっているかどうかを確認しています

S3オブジェクトロックが有効になっているかどうかを確認するには、GET Object Lock Configuration要求を使用します。

"バケットの処理"

S3オブジェクトのロック設定を使用してオブジェクトを作成する

S3 オブジェクトロックが有効になっているバケットにオブジェクトのバージョンを追加するときに S3 オブジェクトのロック設定を指定するには、PUT Object、PUT Object - Copy、Initiate Multipart Upload 要求のいずれかを実行します。次の要求ヘッダーを使用します。



バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。

- `x-amz-object-lock-mode` は、コンプライアンスに準拠している必要があります（大文字と小文字が区別されます）



を指定する場合 `x-amz-object-lock-mode`、も指定する必要があります `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
 - `retain-until-date` の値は、`YYYY-MM-DDTHH:MM:SSZ` の形式で指定する必要があります。秒数には分数を指定できませんが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
 - `retain-until-date` は将来の日付にする必要があります。
- `x-amz-object-lock-legal-hold`

リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、400 Bad Request（InvalidArgument）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- `Content-MD5` 要求ヘッダーがある場合は必須です `x-amz-object-lock-*` 要求ヘッダーが PUT Object 要求に含まれています。Content-MD5 PUT Object - Copy または Initiate Multipart Upload には必要ありません。
- バケットで S3 オブジェクトロックが有効になっていない場合は、`x-amz-object-lock-*` 要求ヘッダーが存在し、400 Bad Request（InvalidRequest）エラーが返されます。
- PUT Object 要求では、`x-amz-storage-class: REDUCED_REDUNDANCY` の使用がサポートされます。AWS の動作に合わせて調整できます。ただし、S3 オブジェクトのロックが有効になっているバケットにオブジェクトが取り込まれると、StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続の GET または HEAD Object バージョンの応答では、ヘッダーが含まれます `x-amz-object-lock-mode`、`x-amz-object-lock-retain-until-date` および `x-amz-object-lock-legal-hold` が設定されている場合、および要求の送信者が正しいかどうか `s3:Get*` 権限：
- それ以降の DELETE Object version 要求または DELETE Objects versions 要求は、`retain-until` 日の前であるか、リーガルホールドがオンの場合には失敗します。

S3オブジェクトのロック設定を更新しています

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- PUT Object legal-hold

新しいリーガルホールドの値が on の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- PUT Object retention

- モード値は準拠している必要があります（大文字と小文字が区別されます）。
- retain-une-dateの値は、の形式で指定する必要があります 2020-08-10T21:46:00z。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
- オブジェクトバージョンに既存の retain-until がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["テナントアカウントを使用する"](#)

["PUT Object の場合"](#)

["PUT Object - Copy の各コマンドを実行します"](#)

["マルチパートアップロードを開始します"](#)

["オブジェクトのバージョン管理"](#)

["Amazon Simple Storage Service User Guide : Using S3 Object Lock"](#)

サーバ側の暗号化を使用

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE（StorageGRID で管理されるキーによるサーバ側の暗号化）*：オブジェクトを格納する S3 要求を問題 で暗号化すると、StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C（ユーザ指定のキーによるサーバ側の暗号化）*：オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。



SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

SSEを使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

`x-amz-server-side-encryption`

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します

SSE-Cを使用する

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

要求ヘッダー	説明
<code>x-amz-server-side-encryption-customer-algorithm</code>	暗号化アルゴリズムを指定します。ヘッダー値はある必要があります AES256。
<code>x-amz-server-side-encryption-customer-key</code>	オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、Base64 でエンコードされた 256 ビットである必要があります。
<code>x-amz-server-side-encryption-customer-key-MD5</code>	RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、Base64 でエンコードされた 128 ビットである必要があります。

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- オブジェクトの取得
- HEAD Object の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します

- パーツをアップロードします
- パーツのアップロード - コピー

ユーザ指定のキーによるサーバ側の暗号化（SSE-C）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。



SSE-C を使用すると、http 経由の要求が StorageGRID ですべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットに CloudMirror レプリケーションが設定されている場合は、SSE-C オブジェクトを取り込むことができません。取り込み処理は失敗します。

関連情報

["オブジェクトの取得"](#)

["HEAD Object の実行"](#)

["PUT Object の場合"](#)

["PUT Object - Copy の各コマンドを実行します"](#)

["マルチパートアップロードを開始します"](#)

["パーツをアップロードします"](#)

["パーツのアップロード - コピー"](#)

["Amazon S3 開発者ガイド：「お客様が用意した暗号化キーによるサーバ側の暗号化（SSE-C）を使用したデータの保護」"](#)

オブジェクトの取得

S3 GET Object 要求を使用して、S3 バケットからオブジェクトを読み出すことができ

ます。

PartNumber要求パラメータはサポートされていません

。 partNumber 要求パラメータはGET Object要求ではサポートされません。マルチパートオブジェクトの特定のパートを読み出すGET要求は実行できません。501 Not Implementedエラーが返され、次のメッセージが表示されます。

```
GET Object by partNumber is not implemented
```

ユーザ指定の暗号化キーによるサーバ側の暗号化（SSE-C）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、3つのヘッダーをすべて使用します。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key:オブジェクトの暗号化キーを指定します
- x-amz-server-side-encryption-customer-key-MD5:オブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前にサーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の UTF-8 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対してGET要求を実行した場合、からは返されません x-amz-missing-meta キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません XNotImplemented :

- x-amz-website-redirect-location

バージョン管理

の場合 versionId サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。

クラウドストレージプールオブジェクトに対する GET Object の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、GET Object 要求の動作はオブジェクトの状態によって異なります。詳細については、「head Object」を参照してください。



オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに1つ以上存在する場合、GET Object 要求はクラウドストレージプールからデータを読み出す前に、グリッドからデータを読み出そうとします。

オブジェクトの状態	GET Object の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK オブジェクトのコピーが読み出されます。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK オブジェクトのコピーが読み出されます。
オブジェクトを読み出し不可能な状態に移行した	403 Forbidden、 InvalidObjectState POST Object restore 要求を使用して、オブジェクトを読み出し可能な状態にリストアします。
読み出し不可能な状態からリストア中である	403 Forbidden、 InvalidObjectState POST Object restore 要求が完了するまで待ちます。
クラウドストレージプールへのリストアが完了している	200 OK オブジェクトのコピーが読み出されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。GET Object 要求が誤って返されることがあります 200 OK オブジェクトの一部のパーツがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパーツがまだリストアされていない場合。

このような場合は、次のよう

- GET Object 要求がデータの一部を返し、転送の途中で停止することがあります。
- 後続のGET Object要求が返されることがあります 403 Forbidden。

関連情報

["サーバ側の暗号化を使用"](#)

["ILM を使用してオブジェクトを管理する"](#)

"POST Object restore の実行"

"監査ログで追跡される S3 処理"

HEAD Object の実行

S3 HEAD Object 要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、HEAD Object を使用してオブジェクトの移行状態を特定できます。

ユーザ指定の暗号化キーによるサーバ側の暗号化（**SSE-C**）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-server-side-encryption-customer-key`: オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`: オブジェクトの暗号化キーの MD5 ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に、サーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対して HEAD 要求を実行しても、は返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented` :

- `x-amz-website-redirect-location`

クラウドストレージプールオブジェクトの応答ヘッダー

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、次の応答ヘッダーが返されます。

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされる時の状態に関する情報を提供します。

オブジェクトの状態	HEAD Object への応答
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK (特別な応答ヘッダーは返されません)。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>オブジェクトが読み出し不可能な状態に移行されるまでの間、の値 expiry-date は、将来の特定の日に設定されます。移行の正確な時間は、StorageGRID システムでは制御されません。</p>
オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>の値 expiry-date は、将来の特定の日に設定されます。</p> <ul style="list-style-type: none"> 注：グリッド上のコピーを取得できない場合（ストレージノードが停止している場合など）は、オブジェクトを読み出す前に、問題 a POST Object restore 要求を実行してクラウドストレージプールからコピーをリストアする必要があります。
読み出し不可能な状態に移行しており、グリッドにコピーが存在しない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
読み出し不可能な状態からリストア中である	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

オブジェクトの状態	HEAD Object への応答
クラウドストレージプールへのリストアが完了している	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" 。 expiry-date クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。</pre>

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。HEAD Object 要求が誤って返されることがあります `x-amz-restore: ongoing-request="false"` オブジェクトの一部のパーツがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパーツがまだリストアされていない場合。

バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

関連情報

["サーバ側の暗号化を使用"](#)

["ILM を使用してオブジェクトを管理する"](#)

["POST Object restore の実行"](#)

["監査ログで追跡される S3 処理"](#)

POST Object restore の実行

S3 POST Object restore 要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

サポートされている要求タイプ

StorageGRID では、オブジェクトのリストアに POST Object restore 要求のみがサポートされます。ではサポートされません SELECT リストアのタイプ。戻り要求を選択してください XNotImplemented。

バージョン管理

必要に応じて、と指定します `versionId` バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアする。指定しない場合は ``versionId`` オブジェクトの最新バージョンがリストアされます

クラウドストレージプールオブジェクトでの **POST Object restore** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、POST Object restore 要求はオブジェクトの状態に基づいて次のように動作します。詳細については、「head Object」を参照してください。



オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合は、POST Object restore 要求を実行してオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

オブジェクトの状態	POST Object restore の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない	403 Forbidden、InvalidObjectState
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK 変更は行われません。 *注：読み出し不可能な状態に移行する前に、オブジェクトを変更することはできません expiry-date。
オブジェクトを読み出し不可能な状態に移行した	202 Accepted 要求の本文で指定されている日数、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。 必要に応じて、を使用します Tier リストアジョブの完了までにかかる時間を確認するための要求要素 (Expedited、Standard`または`Bulk)。指定しない場合は Tier、Standard 階層を使用しています。 *注意：S3 Glacier Deep Archiveまたはクラウドストレージプールに移行されたオブジェクトや、Azure Blob Storageを使用するクラウドストレージは、を使用してリストアできません Expedited 階層：次のエラーが返されます 403 Forbidden、InvalidTier : Retrieval option is not supported by this storage class。
読み出し不可能な状態からリストア中である	409 Conflict、RestoreAlreadyInProgress

オブジェクトの状態	POST Object restore の動作
クラウドストレージプールへのリストアが完了している	200 OK *注：*オブジェクトが読み出し可能な状態にリストアされている場合は、オブジェクトを変更できません expiry-date 用の新しい値を指定してPOST Object restore要求を再発行する Days。要求が実行された日時に基づいてリストア日が更新されます。

関連情報

"ILM を使用してオブジェクトを管理する"

"HEAD Object の実行"

"監査ログで追跡される S3 処理"

PUT Object の場合

S3 PUT Object 要求を使用すると、オブジェクトをバケットに追加できます。

競合の解決

同一キーに書き込む2つのクライアントなど競合するクライアント要求は最新のWINS形式で解決され、最新「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されません。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない）UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、PUT、PUT Object-Copy、GET、HEAD の各要求は正常に実行されます。
- StorageGRID から返されない x-amz-missing-meta キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Cache-Control
- Content-Disposition
- Content-Encoding

を指定する場合 `aws-chunked` の場合 `Content-Encoding` StorageGRID では、次の項目は検証されません。

- StorageGRID ではが検証されません `chunk-signature` チャンクデータに対して。
- StorageGRID は、ユーザが指定した値を検証しません `x-amz-decoded-content-length` をクリックします。

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

チャンク転送エンコードは、の場合にサポートされます `aws-chunked` ペイロード署名も使用されます。

- ``x-amz-meta-`` をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します。

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-name: value
```

ILMルールの参照時間として `* User Defined Creation Time *` オプションを使用する場合は、を使用する必要があります `creation-time` を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 `creation-time` は、1970年1月1日からの秒数として評価されます。



ILM ルールで、参照時間に * User Defined Creation Time * と取り込み動作に `Balanced` オプションまたは `Strict` オプションの両方を使用することはできません。ILM ルールの作成時にエラーが返されます。

- `x-amz-tagging`
- S3 Object Lock 要求のヘッダー
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

"S3 REST API のサポートされる処理と制限事項"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `x-amz-acl` 要求ヘッダーはサポートされていません。
- `x-amz-website-redirect-location` 要求ヘッダーはサポートされておらず、返されます `XNotImplemented`。

ストレージクラスのオプション

◦ `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class StorageGRID` が取り込み中にオブジェクトデータを保護する方法に影響し、`StorageGRID` システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールの取り込み動作が`Strict`オプションに指定されている場合、はを使用します `x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class` :

- STANDARD (デフォルト)

- *** Dual commit *** : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます (デュアルコミット)。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
- *** Balanced *** : ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

StorageGRID が ILM ルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合 (同期配置) は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

- **REDUCED_REDUNDANCY**

- *** Dual commit *** : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します (シングルコミット)。
- *** Balanced *** : ILM ルールで Balanced オプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。
REDUCED_REDUNDANCY オプションは、オブジェクトに一致する ILM ルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- **注意 *** : 一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納されるときに冗長性レベルが低下することはありません。

***注 :** S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- *** SSE *** : StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
 - `x-amz-server-side-encryption`
- *** SSE-C *** : ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つのヘ

ッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します AES256。
 - `x-amz-server-side-encryption-customer-key`:新しいオブジェクトの暗号化キーを指定します。
 - `x-amz-server-side-encryption-customer-key-MD5`:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。
- 注意：* 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

*注：SSEまたはSSE-Cで暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、nullバージョンがすでに存在する場合は上書きされます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["バケットの処理"](#)

["監査ログで追跡される S3 処理"](#)

["サーバ側の暗号化を使用"](#)

["クライアント接続の設定方法"](#)

PUT Object - Copy の各コマンドを実行します

S3 PUT Object - Copy 要求を使用すると、すでに S3 に格納されているオブジェクトのコピーを作成できます。PUT Object - Copy 処理は、GET を実行してから PUT を実行する処理と同じです。

競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されません。
- StorageGRID から返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- ``x-amz-meta-`` をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します
- `x-amz-metadata-directive`: デフォルト値は `COPY` をクリックすると、オブジェクトおよび関連するメタデータをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のメタデータを上書きする場合、またはオブジェクトメタデータを更新する場合。

- `x-amz-storage-class`
- `x-amz-tagging-directive`: デフォルト値は `COPY` をクリックすると、オブジェクトとすべてのタグをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のタグを上書きする場合、またはタグを更新する場合。

- S3 オブジェクトロック要求のヘッダー：
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

"サーバ側の暗号化を行うための要求ヘッダー"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

ストレージクラスのオプション

◦ x-amz-storage-class 要求ヘッダーがサポートされ、一致するILMルールで取り込み動作にDual commitまたはBalancedが指定されている場合にStorageGRID で作成されるオブジェクトコピーの数に影響します。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

PUT Object - Copy で x-amz-copy-source を使用しています

ソースのバケットとキーの場合は、で指定します x-amz-copy-source ヘッダーはデスティネーションのバケットおよびキーとは異なり、ソースオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致している場合は、および x-amz-metadata-directive ヘッダーはのように指定します `REPLACE` では、要求で指定されたメタデータの値に基づいてオブジェクトのメタデータが更新されます。この場合、StorageGRID はオブジェクトを再取り込みしません。これには 2 つの重要な結果があります。

- PUT Object - Copy を使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。を用意する場合は x-amz-server-side-encryption ヘッダーまたは x-amz-server-side-encryption-customer-algorithm ヘッダー。StorageGRID は要求を拒否し、戻ります XNotImplemented。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

このため、ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

サーバ側の暗号化を使用する場合は、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって、指定する要求ヘッダーが異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（SSE-C）は、オブジェクトを復号化してコピーできるように、PUT Object - Copy 要求に次の 3 つのヘッダーを含める必要があります。
 - x-amz-copy-source-server-side-encryption-customer-algorithm を指定します AES256。
 - x-amz-copy-source-server-side-encryption-customer-key ソースオブジェクトの作成時に指定した暗号化キーを指定します。
 - x-amz-copy-source-server-side-encryption-customer-key-MD5:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の 3 つのヘッダーを含めます。
 - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-server-side-encryption-customer-key:ターゲットオブジェクトの新しい暗号化キーを指定します
 - x-amz-server-side-encryption-customer-key-MD5:新しい暗号化キーのMD5ダイジェストを指定します。
- 注意：* 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前にサーバ側の暗号化の使用に関する考慮事項を確認してください
- StorageGRID で管理される一意のキーでターゲットオブジェクト（コピー）を暗号化する（SSE）には、PUT Object - Copy 要求に次のヘッダーを含めます。

◦ x-amz-server-side-encryption

注： server-side-encryption オブジェクトの値を更新できません。代わりに、新しいを使用してコピーを作成します server-side-encryption を使用した値 x-amz-metadata-directive： REPLACE。

バージョン管理

ソースバケットがバージョン管理に対応している場合は、を使用できます x-amz-copy-source オブジェクトの最新バージョンをコピーするヘッダー。オブジェクトの特定のバージョンをコピーするには、を使用してコピーするバージョンを明示的に指定する必要があります versionId サブリソース：デスティネーションバケットがバージョン管理に対応している場合は、で生成されたバージョンが返されます x-amz-version-id 応答ヘッダー。ターゲットバケットのバージョン管理が一時停止中の場合は、を実行します x-amz-version-id 「null」 値を返します。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["サーバ側の暗号化を使用"](#)

["監査ログで追跡される S3 処理"](#)

["PUT Object の場合"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。